

Amendment to the Claims:

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

1. (canceled)

2. (currently amended) A method of implementing an elliptic curve cryptographic operation in ~~an~~ a cryptographic apparatus implementing an elliptic curve cryptography in a finite field of characteristic 2 (or an extension field of "2"), in which said elliptic curve is given by $y^2 + xy = ax^2 + b$ and in which x and y are variables in an x - y coordinate system, a and b are parameters, addition of points $P1(x1, y1)$ and $P2(x2, y2)$ on said elliptic curve composed of points defined by individual coordinate components is presumed to be represented by $P3(x3, y3)$ with subtraction of said points $P1(x1, y1)$ and $P2(x2, y2)$ being presumed to be represented by $P4(x4, y4)$, said method comprising the steps performed by said cryptographic apparatus, of:

inputting the coordinate component $x1$;

transforming ~~said the~~ inputted coordinate component $x1$ into x -coordinates and z -coordinates $[X_1, Z_1]$ of a projective space where z is a variable of a projective space where z is a variable in the z -coordinate;

storing said coordinates $[X_1, Z_1]$ of said projective space;

transforming ~~said the~~ coordinate component $x2$ into coordinates $[X_2, Z_2]$ of said projective space;

storing ~~said the~~ projective coordinates $[X_2, Z_2]$;
transforming ~~said the~~ coordinate component x_4 into coordinates $[X_4, Z_4]$ of
said projective space;
storing ~~said the~~ coordinates $[X_4, Z_4]$;
determining projective coordinates $[X_3, Z_3]$ from ~~said the~~ stored projective
coordinates $[X_1, Z_1]$, $[X_2, Z_2]$ and $[X_4, Z_4]$;
transforming said projective coordinates $[X_3, Z_3]$ into ~~said the~~ coordinate
component x_3 ; and
outputting said coordinate component x_3 ,
whereby scalar multiplication of said point $P1 (x_1, y_1)$ is determined;
generating a random number k ;
storing said generated random number k ;
transforming the x - coordinates into projective coordinates to thereby derive
projective coordinates $[k^2x, k]$ through arithmetic operation of individual coordinate
components of said projective space and said stored random number k .

3. (currently amended) A method of implementing an elliptic curve
cryptographic operation in ~~an a cryptographic~~ apparatus implementing an elliptic
curve cryptography in a finite field of characteristic 2 (or an extension field of "2"), in
which said elliptic curve is given by $y^2 + xy = ax^2 + b$ and in which x and y are
variables in an x - y coordinate system, a and b are parameters, addition of points $P1$
(x_1, y_1) and $P2 (x_2, y_2)$ on said elliptic curve composed of points defined by
individual coordinate components is presumed to be represented by $P3 (x_3, y_3)$ with

subtraction of said points P1 (x_1, y_1) and P2 (x_2, y_2) being presumed to be represented by P4 (x_4, y_4), said method comprising the steps performed by said cryptographic apparatus, of:

inputting the coordinate component x_1 ;

transforming ~~said~~ the inputted coordinate component x_1 into x - and z -coordinates [X_1, Z_1] of a projective space where z is a variable of a projective space where z is a variable in the z -coordinate;

storing said coordinates [X_1, Z_1] of said projective space;

transforming ~~said~~ the coordinate component x_2 into coordinates [X_2, Z_2] of said projective space;

storing ~~said~~ the projective coordinates [X_2, Z_2];

transforming ~~said~~ the coordinate component x_4 into coordinates [X_4, Z_4] of said projective space;

storing ~~said~~ the coordinates [X_4, Z_4];

determining projective coordinates [X_3, Z_3] from ~~said~~ the stored projective coordinates [X_1, Z_1], [X_2, Z_2] and [X_4, Z_4];

transforming ~~said~~ the projective coordinates [X_3, Z_3] into said coordinate component x_3 ; and

outputting said coordinate component x_3 ,

whereby scalar multiplication of said point P1 (x_1, y_1) is determined;

generating a random number k ;

storing said generated random number k ;

transforming the x - coordinates into projective coordinates to thereby derive projective coordinates $[kx, k]$ through arithmetic operation of individual coordinate components of said projective space and said stored random number k .

4. - 5. (canceled)

6. (previously presented) An apparatus implementing an elliptic curve cryptographic operation in a finite field of characteristic 2 (or an extension field of "2"), in which x and y are variables in an x - y coordinate system, a and b are parameters, said elliptic curve is given by $y^2 + xy = x^3 + ax^2 + b$, comprising:

random number generating means for generating a random number k ;

projective coordinate transformation means receiving as inputs thereto coordinate x_0 of said finite field of characteristic 2 and said random number k , to thereby transform said coordinate x_0 into projective coordinates $[kx_0, k] = [X_1, Z_1]$;

doubling arithmetic means for arithmetically determining a double point from said projective coordinates $[X_1, Z_1]$;

addition arithmetic means for determining an addition point from said projective coordinate $[X_1, Z_1]$ where Z is a variable in the z -coordinate to thereby output said addition point; and

scalar multiplication means receiving information from said projective coordinate transformation means, said doubling arithmetic means and said addition arithmetic means to thereby perform scalar multiplication of the coordinate component x_0 .

7. (canceled)

8. (currently amended) A recording medium storing a program for implementing an elliptic curve cryptographic operation, said recording medium being in ~~an~~ a cryptographic apparatus implementing an elliptic curve cryptography in a finite field of characteristic 2 (or an extension field of "2"), in which said elliptic curve is given by $y^2 + xy = x^3 + ax^2 + b$, in which x and y are variables in an x - y coordinate system, a and b are parameters, addition of points $P1 (x1, y1)$ and $P2 (x2, y2)$ on said elliptic curve composed of points defined by individual coordinate components is presumed to be represented by $P3 (x3, y3)$ with subtraction of points $P1 (x1, y1)$ and $P2 (x2, y2)$ being presumed to be represented by $P4, (x4, y4)$, said program when executed causing the cryptographic apparatus to perform:

inputting an coordinate component $x1$;

transforming ~~said the~~ inputted coordinate component $x1$ into x - and z -coordinates $[X_1, Z_1]$ in a projective space;

storing said coordinates $[X_2, Z_2]$ of said projective space;

transforming ~~said the~~ coordinate component $x2$ into coordinates $[X_2, Z_2]$ of said projective space;

storing ~~said the~~ projective coordinate $[X_1, Z_1]$ where z is a variable in the z -coordinate;

transforming ~~said the~~ coordinate component $x4$ into coordinates $[X_4, Z_4]$ of said projective space;

storing ~~said~~ the projective coordinates $[X_4, Z_4]$;
determining projective coordinates $[X_3, Z_3]$ from ~~said~~ the stored projective coordinates $[X_1, Z_1]$, $[X_2, Z_2]$ and $[X_4, Z_4]$;
transforming said projective coordinates $[X_3, Z_3]$ into ~~said~~ the coordinate component x_3 ; and
outputting said coordinate component x_3 ,
whereby scalar multiplication of said point $P_1 (x_1, y_1)$ is determined;
generating a random number k ;
storing said generated random number k ;
transforming the x - coordinates into projective coordinates to thereby derive projective coordinates $[k^2x, k]$ through arithmetic operation of individual coordinate components of said projective space and said stored random number k .

9. (currently amended) A recording medium storing a program for implementing an elliptic curve cryptographic operation, said recording medium being in ~~an~~ a cryptographic apparatus implementing an elliptic curve cryptography in a finite field of characteristic 2 (or an extension field of "2"), in which said elliptic curve is given by $y^2 + xy = x^3 + ax^2 + b$, in which x and y are variables in an x - y coordinate system, a and b are parameters, addition of points $P_1 (x_1, y_1)$ and $P_2 (x_2, y_2)$ on said elliptic curve composed of points defined by individual coordinate components is presumed to be represented by $P_3 (x_3, y_3)$ with subtraction of points $P_1 (x_1, y_1)$ and $P_2 (x_2, y_2)$ being presumed to be represented by $P_4 (x_4, y_4)$, said program when executed causing the cryptographic apparatus to perform:

inputting an coordinate component x_1 ;

transforming ~~said-the~~ inputted coordinate component x_1 into x- and z- coordinates $[X_1, Z_1]$ in a projective space;

storing said coordinates $[X_2, Z_2]$ of said projective space;

transforming ~~said-the~~ coordinate component x_2 into coordinates $[X_2, Z_2]$ of said projective space;

storing ~~said-the~~ projective coordinate $[X_1, Z_1]$ where z is a variable in the z-coordinate;

transforming ~~said-the~~ coordinate component x_4 into coordinates $[X_4, Z_4]$ of said projective space;

storing ~~said-the~~ projective coordinates $[X_4, Z_4]$;

determining projective coordinates $[X_3, Z_3]$ from ~~said-the~~ stored projective coordinates $[X_1, Z_1]$, $[X_2, Z_2]$ and $[X_4, Z_4]$;

transforming said projective coordinates $[X_3, Z_3]$ into ~~said-the~~ coordinate component x_3 ; and

outputting said coordinate component x_3 ,

whereby scalar multiplication of said point $P_1 (x_1, y_1)$ is determined;

generating a random number \underline{k} ;

storing said generated random number \underline{k} ;

transforming the x- coordinates into projective coordinates to thereby derive projective coordinates $[kx, k]$ through arithmetic operation of individual coordinate components of said projective space and said stored random number \underline{k} .

U.S. Application No. 09/468,948

10. - 12. (canceled)